WHAT IS CLAIMED IS:

1. A method of operating an integrated circuit with on-chip volatile program memory comprising:

inputting a stream of data comprising unencrypted configuration data to the integrated circuit;

encrypting the unencrypted configuration data using a security circuit of the integrated circuit and a security key stored in the integrated circuit; and

outputting a stream of encrypted configuration data from the integrated circuit.

2. The method of claim 1 wherein the stream of data is input serially.

3. The method of claim 1 comprising:

configuring the integrated circuit using the unencrypted configuration data.

4. The method of claim 1 comprising:

storing the stream of encrypted configuration data in a nonvolatile storage device.

5. The method of claim 4 comprising:

inputting the stream of encrypted configuration data from the nonvolatile storage device to the integrated circuit;

decrypting the encrypted configuration data using the security circuit of the integrated circuit and the security key; and

configuring the integrated circuit with a decrypted version of the encrypted configuration data.

6. The method of claim 1 wherein the stream of configuration data includes a header indicating the configuration data is unencrypted.

7. The method of claim 5 wherein the stream of encrypted configuration data includes a header indicating the configuration data is encrypted.

8. The method of claim 1 comprising:

generating the security key using a random number generator circuit of the integrated circuit.

9. The method of claim 1 comprising:

storing the security key in a device ID register of the integrated circuit.

10. The method of claim 1 wherein the stream of configuration data comprises preamble, header, initial value, configuration data, and message authentication code portions.

11. The method of claim 9 wherein the ID register is nonvolatile.

12. The method of claim 1 wherein the unencrypted configuration data has approximately the same number of bits as the encrypted configuration data.

13. The method of claim 8 further comprising:

storing the security key in a device ID register of the integrated circuit.

14. The method of claim 10 wherein information in the preamble indicates whether the configuration data of the stream is encrypted or unencrypted.

15. The method of claim 10 wherein based on the preamble, the integrated circuit can determine whether the stream of data is for a previous version of the programmable gate array, without a security scheme, or the stream of data is for a version of the integrated circuit with the security scheme.

16. The method of claim 10 wherein using the preamble, a integrated circuit with a security scheme will be backwards compatible with versions of the integrated circuit without the security scheme.

17. The method of claim 10 comprising:

when the preamble is a first value, processing the stream of data as a stream of data for a version of the integrated circuit without a security scheme; and

when the preamble is a second value, different from the first value, processing the stream of data as a stream of data for a version of the integrated circuit with the security scheme.

18. The method of claim 9 wherein the ID register is backed up using an external battery.

19. The method of claim 1 wherein the stream of data is loaded using a JTAG interface of the integrated circuit.

20. The method of claim 1 wherein the stream of data is provided using a microprocessor.

21. The method of claim 1 comprising:

receiving the stream of encrypted configuration data using a microprocessor.

22. The method of claim 21 comprising:

using the microprocessor, writing the encrypted configuration data into a nonvolatile storage device.

23. The method of claim 4 wherein the nonvolatile storage device is a serial EPROM or serial EEPROM.

24. The method of claim 4 wherein the nonvolatile storage device is a Flash memory.

25. The method of claim 11 wherein the ID register comprises floating-gate transistors.

26. The method of claim 11 wherein the ID register comprises fuses.

27. The method of claim 11 wherein the ID register comprises antifuses.

28. The method of claim 11 wherein the ID register is programmed during manufacture of the integrated circuit.

29. The method of claim 28 wherein the ID register is programmed using a laser.

30. The method of claim 28 wherein the ID register is programmed using a high voltage.

31. The method of claim 18 wherein the external battery is coupled to a first power supply terminal to the ID register, and a second power supply terminal for non-backed up circuits is not coupled to the external battery.

32. The method of claim 1 wherein the security key has a fixed value and further comprising:

generating an initial value for the security circuit; and

outputting the initial value from of the integrated circuit.

33. The method of claim 32 wherein the unencrypted configuration data is encrypted using the initial value.

34. The method of claim 32 wherein the initial value is generated using a random number generator.

35. The method of claim 1 wherein the security circuit encrypts the unencrypted configuration data using a triple data encryption standard in a cipher block chaining mode algorithm.

36. The method of claim 11 wherein the device ID register is implemented using an error correcting code scheme.

37. A method of operating a integrated circuit comprising:

receiving first encrypted configuration data and a first security key from a network;

decrypting the first encrypted configuration data to obtain unencrypted configuration data using a first security key using user programmed circuitry of the integrated circuit; and

encrypting the unencrypted configuration data using a second security key and a fixed security circuit of the integrated circuit to obtain second encrypted configuration data.

38. The method of claim 37 further comprising:

outputting the second encrypted configuration data from the integrated circuit.

39. The method of claim 38 further comprising:

storing the second encrypted configuration data in a nonvolatile storage device.

40. The method of claim 39 wherein the nonvolatile storage device is a serial EPROM.

41. The method of claim 37 wherein the second security key is stored in an ID register of the integrated circuit.

42. The method of claim 37 wherein the configured user logic outputs the unencrypted configuration data to the security circuit using an on-chip interconnection.

43. The method of claim 37 further comprising:

configuring the integrated circuit using the unencrypted configuration data.

44. The method of claim 37 wherein the first encrypted configuration data is serially transferred to an I/O pin of the integrated circuit.

45. The method of claim 37 wherein the security circuit encrypts the unencrypted configuration data using a triple data encryption standard (DES) in a cipher block chain (CBC) mode algorithm.

46. A field programmable gate array comprising:

a serial interface for loading initial configuration and key information;

a battery-backed on-chip memory for storing the cryptographic key;

a triple-DES encryption circuit; and

an interface to an external nonvolatile memory for storing encrypted configuration data.

47. A method for securely configuring an FPGA comprising:

loading key information into an on-chip battery-backed register;

loading an initial configuration through a JTAG interface; and

storing an encrypted version of the configuration in an external nonvolatile memory.

48. A field programmable gate array comprising:

a plurality of static random access memory cells to store a configuration of user-configurable logic of the field programmable gate array;

an ID register to store a security key; and

a decryption circuit to receive and decrypt a stream of encrypted configuration data using the security key, and generate decrypted configuration data for configuring the static random access memory cells.

49. The field programmable gate array of claim 48 further comprising:

a first positive supply input pin coupled to the static random access memory cells, user-configurable logic, and decryption circuit; and

a second positive supply input pin coupled to the ID register, wherein the second positive supply input is to be coupled to an external backup battery.

50. The field programmable gate array of claim 49 wherein when power is removed from the first positive supply input pin, the configuration of the static random access memory cells is erased, and the security key stored in the ID register is maintained by the external backup battery.

51. The field programmable gate array of claim 50 wherein the external backup battery only supplies power to the ID register.

52. The field programmable gate array of claim 48 wherein the decryption circuit decrypts the stream of encrypted configuration data using a triple-DES algorithm.

53. The field programmable gate array of claim 49 further comprising:

a random number generator circuit to generate the security key.

54. The field programmable gate array of claim 51 wherein a current draw on the external backup battery is about a microamp or less.

55. The field programmable gate array of claim 51 wherein current draw on the external backup battery is about 10 microamps or less.